Chameleon

Mode d’emploi

powered by

LucidPORT

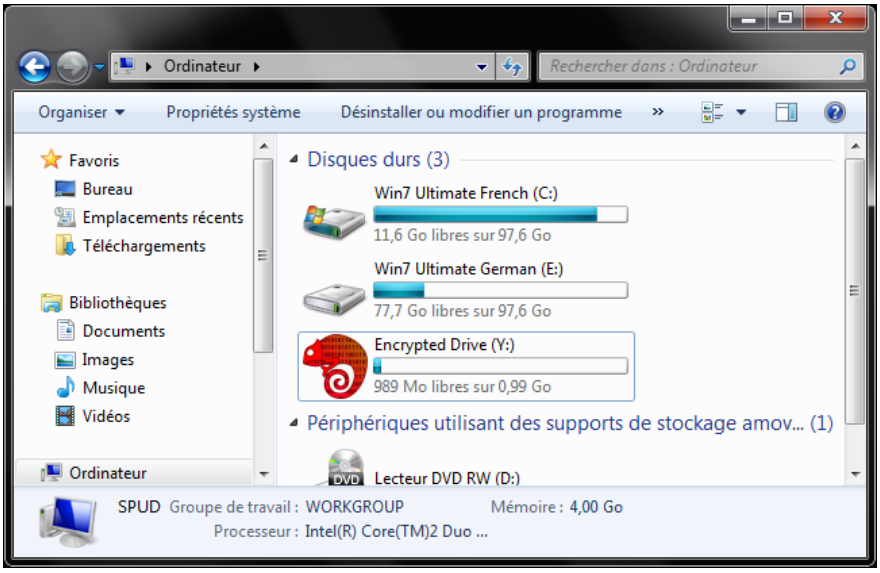
Table des matières

1 Introduction 2
2 Installation et réglages 2
2.1 Désinstaller 5
3 Disques cryptés Chameleon : protéger vos données 5
4 Crypter des fichiers et dossiers individuels 8
4.1 Crypter des fichiers et dossiers individuels 8
4.2 Décrypter des fichiers 11
4.3 Voir les détails d'un fichier crypté 14
5 Dupliquer un dispositif Chameleon 15
6 Désactiver des dispositifs Chameleon égarés 16
6.1 Faire migrer des fichiers cryptés (.cge) 18
7 Protection par mot de passe 19
7.1 Modification du mot de passe 19
8 Ajouter, supprimer et modifier la taille des disques cryptés 21
9 Fonctions supplémentaires et restrictions 22
9.1 Utilisation d'un dispositif Chameleon à partir de plusieurs ordinateurs 22
9.2 Utilisation de plusieurs dispositifs Chameleon sur le même ordinateur 23
9.3 Fichier Windows de Pagination 23
9.4 Retirer le dispositif de façon sécurisée 24
9.5 Créer des copies de sauvegarde des données 25
10 Garantie limitée et Mentions Légales 25

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

1 Introduction

Le Chameleon Pro protège les fichiers de votre PC grâce à un cryptage AES-256. Contrairement aux autres dispositifs USB de cryptage, Chamelon Pro protège les fichiers sur le disque dur au lieu de les transférer vers un dispositif USB. Le Chameleon Pro créé un disque crypté en utilisant l'espace libre de votre disque dur. Les fichiers et applications enregistrés sur ce disque crypté sont protégés et on ne peut y avoir accès que lorsque le dispositif Chameleon est connecté. Tout comme votre clé de voiture, le dispositif agit en tant que clé matérielle pour votre disque dur.



Le Chameleon Pro fonctionne sur les PC équipés de Windows XP, Vista et Win7.

2 Installation et réglages

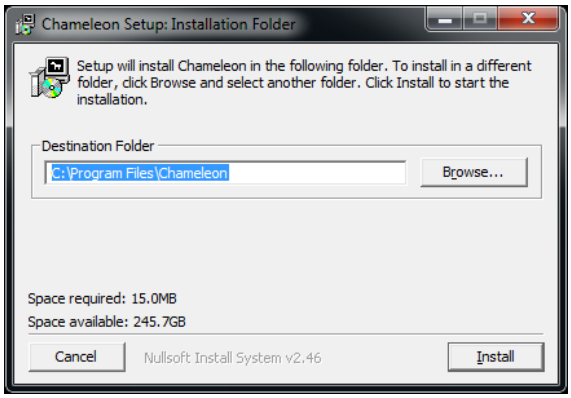
1. Avant d'installer le logiciel Chameleon, vérifiez que toutes les versions précédentes du Chameleon soient bien désinstallées. La désinstallation ne supprime pas les disques cryptés existants.

2. **Insérez le CD d'installation** et **exécutez le programme Installation**.[1] (Vous pouvez également télécharger le programme d'installation sur : http:// www.zepla.fr/telechargement.)

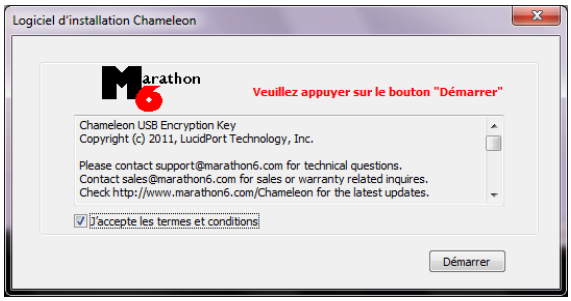
[1] Sur certains ordinateurs fonctionnant sous Windows7, il se peut que vous receviez un avertissement du Contrôle de Compte Utilisateur vous informant qu'un programme essaye d'effectuer des changements sur votre ordinateur. Dans ce cas, sélectionnez « Oui » ou « Installer ».

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

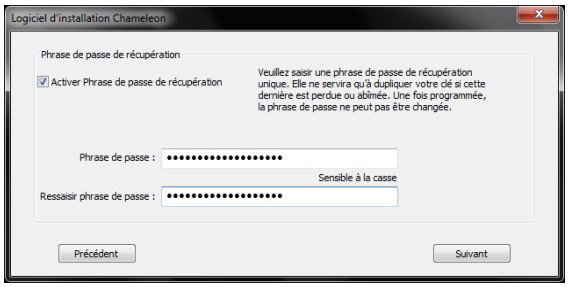
3. **Cliquez sur le bouton « Installer »** pour charger le logiciel.


Chameleon Setup: Installation Folder
Setup will install Chameleon in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files\Chameleon
Browse...
Space required: 15.0MB
Space available: 245.7GB
Cancel
Nullsoft Install System v2.46
Install

4. **Insérer le dispositif Chameleon** puis **cliquez sur « Démarrer »** pour lancer l'assistant à l'installation.


Logiciel d'installation Chameleon
Marathon
Veuillez appuyer sur le bouton "Démarrer"
Chameleon USB Encryption Key
Copyright (c) 2011, LucidPort Technology, Inc.
Please contact support@marathon6.com for technical questions.
Contact sales@marathon6.com for sales or warranty related inquires.
Check http://www.marathon6.com/Chameleon for the latest updates.
J'accepte les termes et conditions
Démarrer

5. **Choisissez entre A), B), ou C)**


Logiciel d'installation Chameleon
Phrase de passe de récupération
Activer Phrase de passe de récupération
Veuillez saisir une phrase de passe de récupération unique. Elle ne servira qu'à dupliquer votre clé si cette dernière est perdue ou abîmée. Une fois programmée, la phrase de passe ne peut pas être changée.
Phrase de passe :
Sensible à la casse
Ressaisir phrase de passe :
Précédent
Suivant

A) Choisissez une phrase de passe de récupération. Cette phrase de passe est utilisée uniquement pour créer des doubles de votre dispositif Master (au cas où vous le perdriez) et n'est pas utilisée en fonctionnement normal. Vous pouvez voir votre phrase de passe de récupération comme un mot de passe sauvegardé dans le dispositif lui-même.

Sélectionnez une phrase de passe unique. Il est possible qu'un autre dispositif Chameleon ayant la même phrase de passe accède à vos données. Une fois programmée, la phrase de passe de récupération ne peut jamais être changée.

Pour être efficace, une phrase de passe devrait faire au moins 16 caractères de long et inclure des lettres aléatoires (majuscules et minuscules), des chiffres et des symboles spéciaux. Protégez votre phrase de passe comme vous protégeriez un mot de passe. Un assaillant qui prendrait connaissance de votre phrase de passe pourrait l'utiliser pour créer le double d'un dispositif. Il n'existe aucun moyen de dupliquer un dispositif Chameleon sans votre phrase de passe de récupération.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

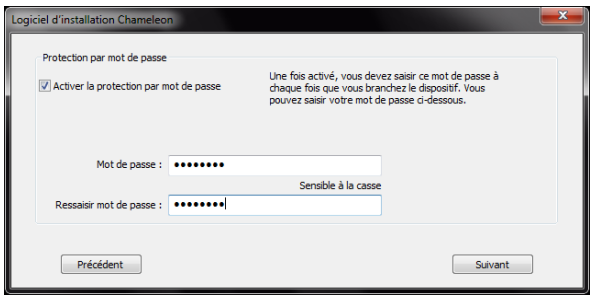
B) Pour un équilibre optimal entre sécurité et redondance, utilisez une séquence aléatoire d'au moins 64 chiffres et lettres comme phrase de passe. Une fois l'installation terminée, créez plusieurs doubles du dispositif avec cette séquence, comme copies de sauvegarde. (Voir « `5 Dupliquer un dispositif Chameleon` »). Afin de pouvoir créer des doubles supplémentaires à l'avenir, sauvegardez la séquence aléatoire dans un emplacement sûr. Sinon, supprimez la séquence.

C) Désactivez la phrase de passe de récupération. Pour une sécurité maximum, désactivez la phrase de passe de récupération. Ceci donne l'ordre au dispositif de générer sa propre clé de cryptage aléatoire. Cela signifie cependant que vous ne pourrez pas dupliquer ou remplacer le dispositif s'il est perdu ou endommagé.

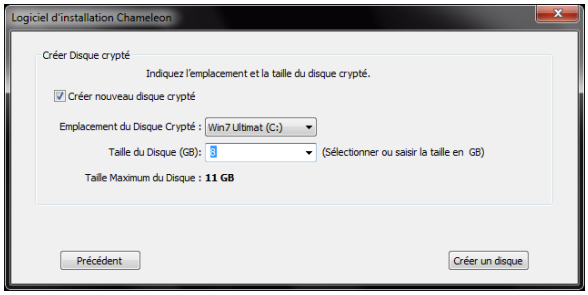
Logiciel d'installation Chameleon
Phrase de passe de récupération
Activer Phrase de passe de récupération
Veuillez saisir une phrase de passe de récupération unique. Elle ne servira qu'à dupliquer votre clé si cette dernière est perdue ou abîmée. Une fois programmée, la phrase de passe ne peut pas être changée.
Phrase de passe :
Sensible à la casse
Ressaisir phrase de passe :
Précédent
Suivant

6. **Activez/Désactivez le mot de passe.** Une fois activé, le mot de passe doit être saisi à chaque fois que vous connectez l'appareil. Un mot de passe n'est pas obligatoire et peut être ajouté ou modifié à n'importe quel moment.

   Une fois activé, le mot de passe doit être différent de la phrase de passe de récupération. Un mot de passe protège votre dispositif Chameleon contre toute utilisation non autorisée.


Logiciel d'installation Chameleon
Protection par mot de passe
Activer la protection par mot de passe
Une fois activé, vous devez saisir ce mot de passe à chaque fois que vous branchez le dispositif. Vous pouvez saisir votre mot de passe ci-dessous.
Mot de passe :
Sensible à la casse
Ressaisir mot de passe :
Précédent
Suivant

7. **Créez un disque crypté.** Indiquez la taille et l'emplacement du disque. Le logiciel d'installation créé le disque crypté en utilisant l'espace libre à cet emplacement. Il peut résider sur votre disque dur local ou sur des disques USB externes. Sa taille peut être modifiée ultérieurement.


Logiciel d'installation Chameleon
Créer Disque crypté
Indiquez l'emplacement et la taille du disque crypté.
Créer nouveau disque crypté
Emplacement du Disque Crypté :
Win7 Ultimat (C:)
Taille du Disque (GB):
(Sélectionner ou saisir la taille en GB)
Taille Maximum du Disque : 11 GB
Précédent
Créer un disque

La totalité du contenu copié sur le disque crypté est protégée automatiquement. Elle est accessible lorsque le dispositif est inséré et disparaît lorsque le dispositif est retiré.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

2.1 Désinstaller

Vous pouvez désinstaller le logiciel Chameleon en localisant « Chameleon » à partir du menu Démarrer de Windows et en sélectionnant « Désinstaller » (Démarrer > Tous les programmes > Chameleon > Désinstaller). La désinstallation ne supprime pas vos disques cryptés. Afin de supprimer des disques cryptés, supprimez le répertoire ChameleonDrives à partir du répertoire de haut niveau de votre disque dur (par ex : C:\ ChameleonDrives\). Le répertoire ChameleonDrives ne peut être supprimé que lorsque le dispositif Chameleon n'est pas connecté.

3 Disques cryptés Chameleon : protéger vos données

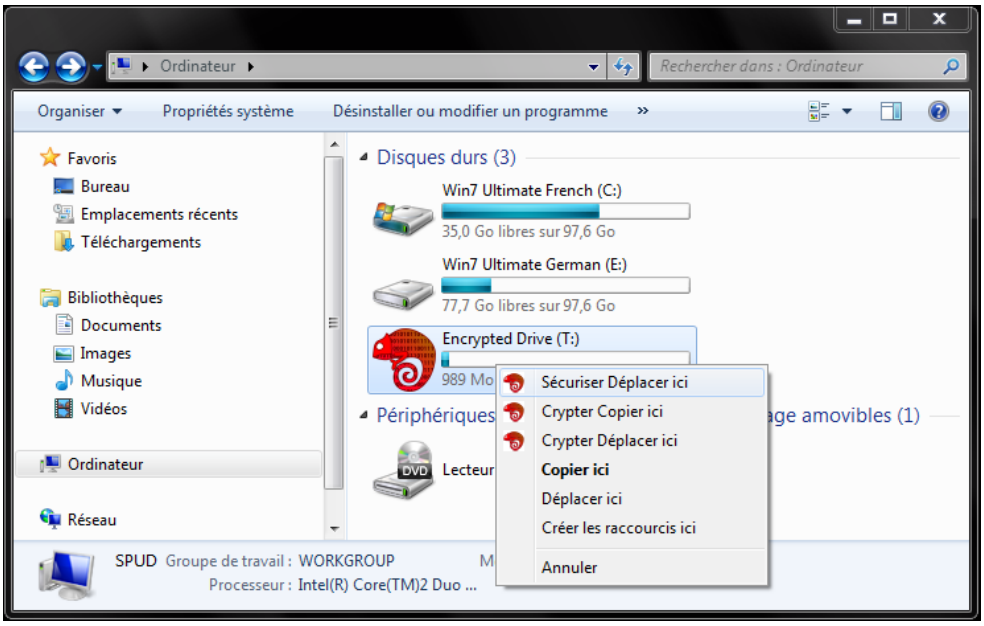
Connectez votre dispositif Chameleon pour accéder au disque crypté. Le disque crypté apparaît comme n'importe quel disque dur sur votre système. Vous pouvez y enregistrer des fichiers, y ouvrir des fichiers, y installer et exécuter des programmes, déplacer des fichiers d'un répertoire à l'autre et indiquer à des applications d'utiliser le disque crypté. Une fois le dispositif Chameleon retiré, le disque crypté disparaît de Windows. Une analyse approfondie de votre disque dur ne révélerait que des données cryptées, d'apparence aléatoire.

Seuls les fichiers enregistrés sur le disque Chameleon sont cryptés. Tout fichier copié ou lu à partir du disque crypté est automatiquement décrypté. Par exemple, si un utilisateur joignait un fichier du disque crypté à un e-mail, ce fichier serait attaché décrypté. Pour la sécurisation des pièces jointes dans les e-mails et du Cloud Storage, voir la rubrique « `4 Crypter des fichiers et dossiers individuels` ».

Vous pouvez copier des fichiers sur le disque crypté en utilisant simplement la commande « glisser-déposer » pour les y déplacer. Cependant, le fichier original non crypté est conservé à son emplacement original. Un « glisser-déposer» effectué avec un clic droit est une méthode plus sécurisée. Maintenez le bouton droit de la souris appuyé, puis faites glisser le fichier sélectionné vers le disque crypté. Une boîte de dialogue apparaîtra alors indiquant « Copier », « Déplacer », et « Sécuriser déplacer ». L'option Sécuriser Déplacer déplace le fichier vers le disque crypté, puis élimine toute trace de ce fichier à son emplacement d'origine.[2] Cela peut prendre un certain temps s'il s'agit d'une quantité de données importante.

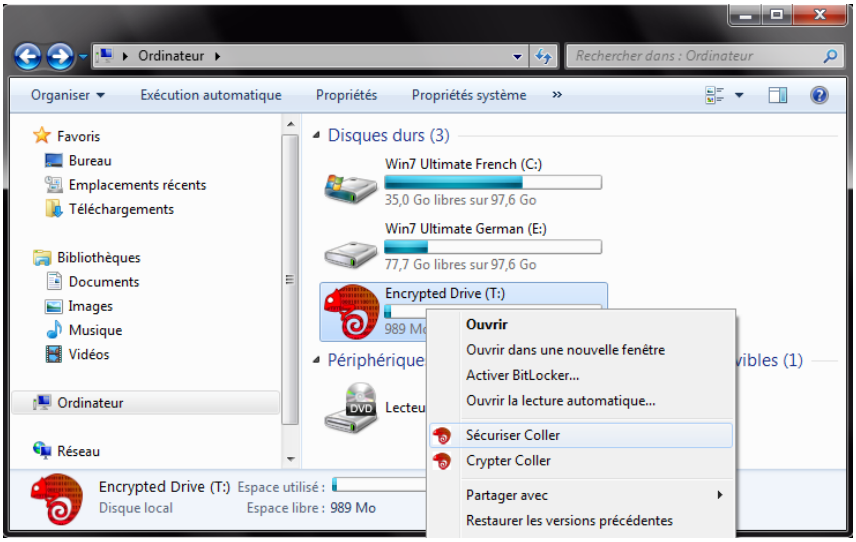
[2] La commande « Déplacer » standard de Windows copie le fichier, puis caractérise le fichier d'origine en tant que fichier supprimé. Il est possible de récupérer le fichier supprimé grâce à des outils spécialisés. L'option « Sécuriser Déplacer » empêche la récupération en écrasant le fichier supprimé.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com



Vous pouvez également déplacer en sécurité un fichier vers le disque crypté en utilisant l'option « Sécuriser Coller ». Faites un clic droit sur le fichier ou dossier que vous souhaitez déplacer, puis sélectionner « Couper ». Ensuite, faites un clic droit sur un disque crypté ou sous-répertoire, puis sélectionnez « Sécuriser Coller ». Tout comme l'option Sécuriser Déplacer, la commande Sécuriser Coller élimine toute trace des fichiers non cryptés sur le disque dur.

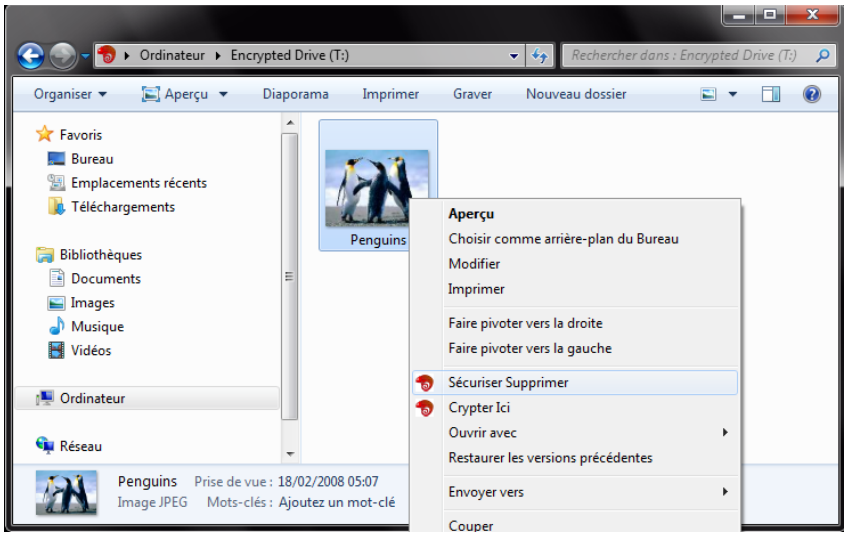
Les commandes « Sécuriser » sont disponibles uniquement lorsque le dispositif Chameleon est connecté.



Le logiciel Chameleon fournit en plus une commande de suppression sécurisée. Faites un clic droit sur un fichier ou dossier puis sélectionnez « Sécuriser Supprimer ». L'utilisation de cette commande est plus sécurisée que la méthode consistant à supprimer le fichier une première fois

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

puis à le supprimer à nouveau dans la corbeille Windows. Puisque la commande « Sécuriser Supprimer » écrase le fichier dans sa totalité absolue à partir du disque dur, s'il s'agit d'une quantité de données importante, l'opération peut prendre un certain temps. Les commandes standards Couper, Coller et Supprimer de Windows restent disponibles.



Lors de sa suppression, un fichier enregistré sur un disque crypté sera déplacé vers la Corbeille Windows. Vous pouvez récupérer le fichier dans la corbeille tant que le dispositif Chameleon reste inséré. Les fichiers supprimés disparaissent de la corbeille lorsque le dispositif est retiré. Ils réapparaissent dans la corbeille lorsque le dispositif est réinséré. Il n'est pas nécessaire d'effectuer la commande « Sécuriser Supprimer » pour les fichiers se trouvant sur le disque crypté.

Tout fichier créé directement sur le disque crypté est automatiquement protégé. Certaines applications cependant, mettent des informations temporaires en mémoire dans votre disque non crypté. Il est possible de récupérer ces informations avec des outils spécialisés. Il est recommandé d'indiquer à vos applications de mettre leurs fichiers temporaires en mémoire dans le disque crypté. Ceci peut généralement se faire en installant vos applications directement sur le disque crypté.

Vous pouvez connecter ou déconnecter le dispositif Chameleon à n'importe quel moment. Votre ordinateur reste entièrement opérationnel même sans le dispositif Chameleon. Seul le disque crypté (ainsi que tous ses programmes et données) sera indisponible. Sachez que si vous débranchez le dispositif alors que les données sont en cours d'écriture au disque crypté, les données risquent d'être corrompues. Cette situation serait similaire à la déconnexion d'un disque dur externe alors qu'il serait en cours d'écriture. Afin d'être absolument certain qu'il n'y ait pas d'écriture en cours, utilisez la fonction « Retirer le périphérique en toute sécurité » de Windows avant de déconnecter le dispositif.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

Si une application est ouverte avec un fichier crypté, cette application et ce fichier peuvent rester accessibles même après que vous ayez déconnecté le dispositif Chameleon. Prenons l'exemple d'un fichier Microsoft Word protégé sur lequel vous seriez en train de travailler. Si vous débranchez le dispositif, une copie de ce fichier reste ouverte dans Word. Vous ne pourrez pas enregistrer ce fichier sur le disque crypté jusqu'à ce que vous réinsériez le dispositif. Vous pouvez cependant visualiser et modifier les parties du fichier présentes en cache dans la mémoire de travail.

4 Crypter des fichiers et dossiers individuels

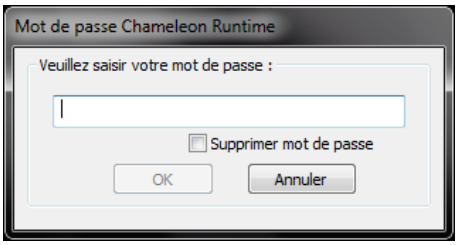
Le dispositif Chameleon crypte automatiquement toutes les données placées dans le disque crypté et décrypte automatiquement toutes les données enlevées du disque crypté. Bien que pratique et sécurisé, ceci ne protège pas les informations envoyées par e-mail ou mises en mémoire sur Internet. Dans de telles situations, le dispositif Chameleon peut crypter et décrypter des fichiers et dossiers individuels.

4.1 Crypter des fichiers et dossiers individuels

Vous pouvez crypter un fichier seul, un groupe de fichiers ou des répertoires entiers (mais pas les raccourcis ou icônes spéciaux comme la corbeille Windows). Les fichiers cryptés par un dispositif Chameleon ne peuvent être décryptés qu'en utilisant le même dispositif (ou par son Master).

1. **Connectez le dispositif**

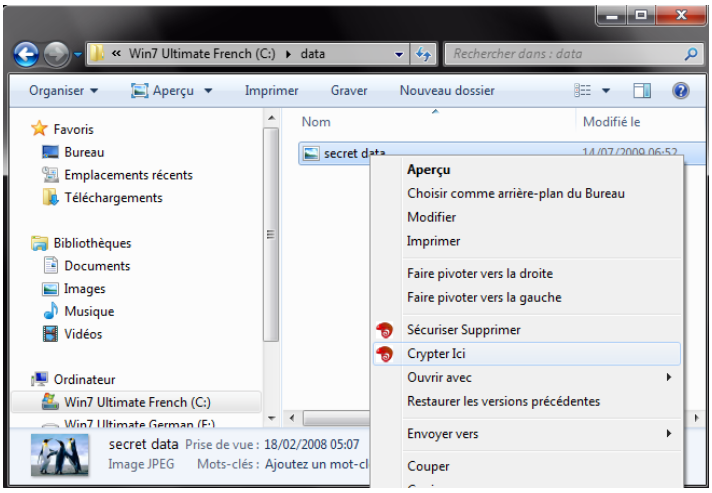
2. **Saisissez votre mot de passe (si activé)**



LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

3. **Faites un clic droit sur le fichier** ou dossier que vous souhaitez protéger

4. **Sélectionnez « Crypter ici »** pour créer une version cryptée du fichier sélectionné

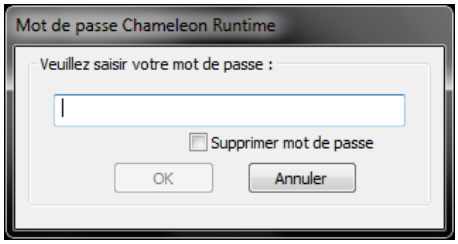


Le fichier crypté apparaîtra comme fichier du même dossier avec le même nom de fichier, mais avec l'extension « .cge ». Si vous le souhaitez, vous pouvez changer le nom du fichier, mais pas l'extension. Ce fichier est crypté grâce au hardware AES-256 du dispositif. Contrairement au disque crypté, le fichier crypté reste visible quand le dispositif est retiré. Il peut être joint à un e-mail, copié vers un disque USB, mis en mémoire dans le réseau ou alors synchronisé à un service Cloud.

Vous pouvez également crypter des fichiers et dossiers individuels en utilisant un « glisser-déposer » effectué avec un clic droit.

1. **Connectez le dispositif**

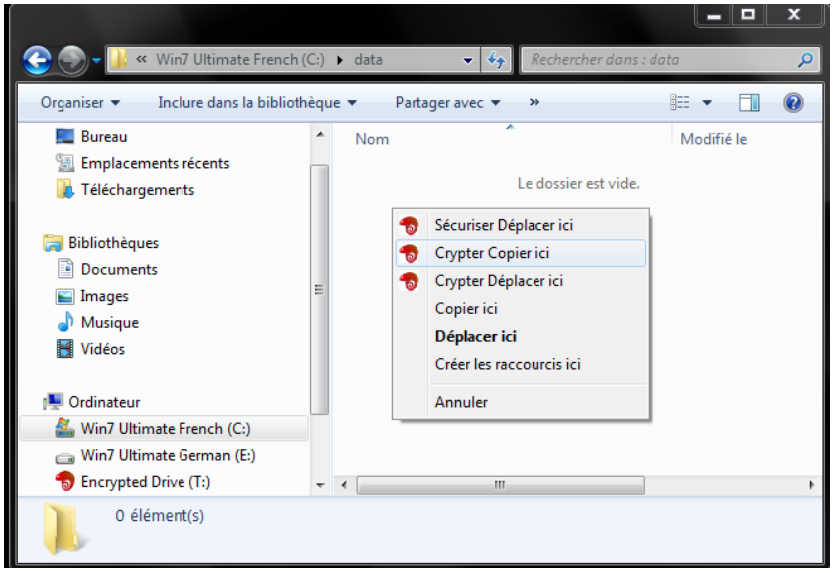
2. **Saisissez votre mot de passe (si activé)**



3. **Cliquez et maintenez appuyé le bouton droit de la souris sur le fichier ou dossier** que vous souhaitez protéger.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

4. **Faites glisser le pointeur de la souris** vers le dossier cible et relâchez le bouton droit de la souris**.** Le fichier crypté sera créé dans ce dossier.



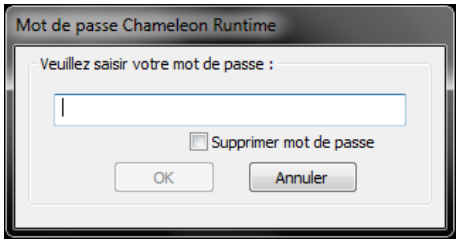
5. **Sélectionnez « Crypter Déplacer ici» ou « Crypter Copier ici»**.
« Crypter Déplacer ici» place le fichier crypté dans l'emplacement choisi tout en supprimant le fichier source en sécurité.

« Crypter Copier ici » fait la même chose, mais sans supprimer le fichier source.

Vous pouvez également crypter un fichier ou dossier en utilisant l'option Crypter Coller :

1. **Connectez le dispositif**

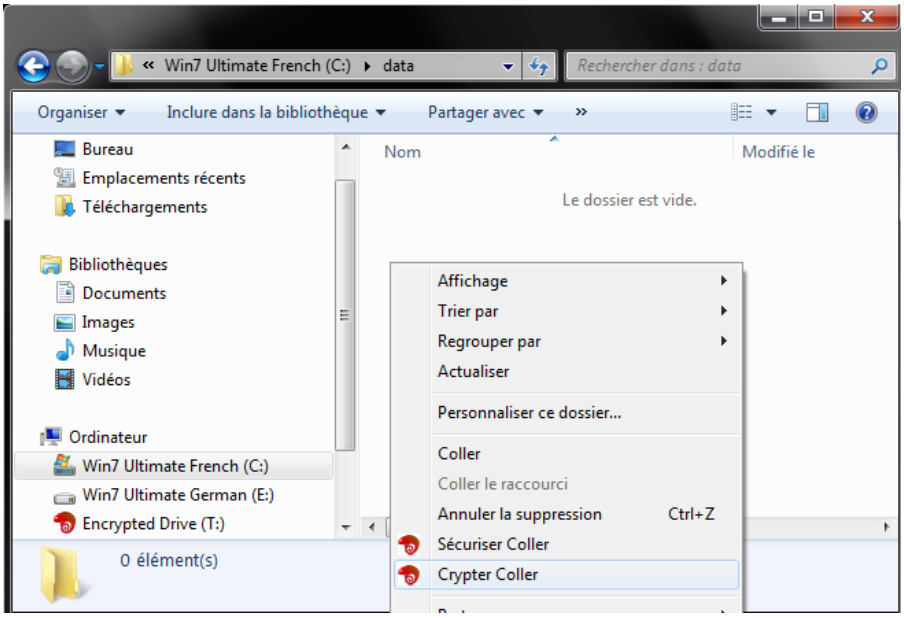
2. **Saisissez votre mot de passe (si activé)**



3. **Faites un clic droit sur le fichier ou dossier** que vous souhaitez crypter, puis **sélectionnez « Couper » ou « Copier »**. Vous pouvez également utiliser les raccourcis du clavier Couper (CTRL+x) ou Copier (CTRL+c).

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

4. **Faites un clic droit le disque ou répertoire de destination.**



1. **Sélectionnez « Crypter Coller »**

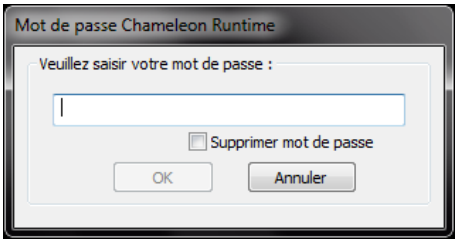
Ceci déplace le fichier crypté vers la destination. Si vous aviez sélectionné « Couper », le fichier source sera supprimé en sécurité une fois le cryptage terminé.

4.2 Décrypter des fichiers

Pour décrypter un fichier .cge :

1. **Connectez le dispositif**

2. **Saisissez votre mot de passe (si activé)**



3. **Double cliquez sur le fichier .cge**.
   Le processus de décryptage commencera immédiatement.

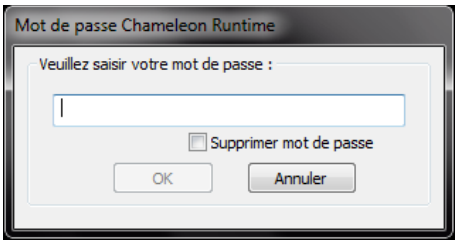
Remarque : si vous ouvrez le fichier .cge à partir d'une application (telle qu'un navigateur Internet) en utilisant (par exemple) « Ouvrir avec », alors le fichier sera téléchargé et décrypté dans un dossier temporaire choisi par l'application. Ceci déplacera le contenu décrypté du fichier .cge dans un dossier imprévu. Au lieu d'ouvrir le fichier .cge directement à partir de l'application, enregistrez-le dans un dossier de votre choix (en utilisant « Enregistrer sous ») et décryptez-le ensuite.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

Les autres méthodes de décryptage de fichiers .cge sont approximativement les mêmes que les méthodes de cryptage :

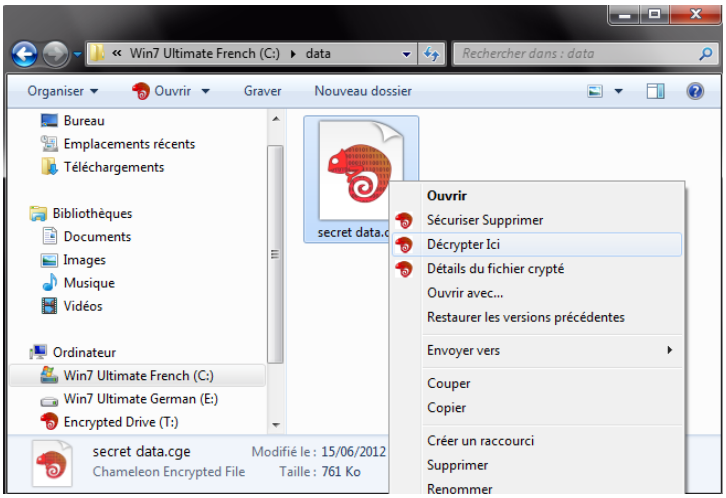
1. **Connectez le dispositif**

2. **Saisissez votre mot de passe (si activé)**



3. **Faites un clic droit sur fichier .cge** à décrypter.

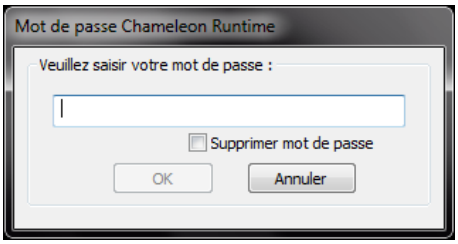
4. **Sélectionnez** « **Décrypter ici** » afin de créer une copie du(des) fichier(s) ou dossier(s) décryptés(s) contenus dans le fichier .cge.



De la même manière, vous pouvez décrypter des fichiers .cge en utilisant la méthode « glisser-déposer » avec un clic droit. Utilisez cette méthode lorsque le fichier .cge se trouve dans une mémoire non sécurisée. Cette méthode est plus fiable car elle permet d'éviter que vos données non cryptées résident (temporairement) dans la mémoire non sécurisée. Prenons l'exemple d'un fichier .cge enregistré sur une unité de réseau. Au lieu de double cliquer sur le fichier afin de le décrypter sur le dossier réseau, vous pouvez utiliser la méthode suivante pour décrypter le fichier sur votre disque dur local.

1. **Connectez le dispositif**

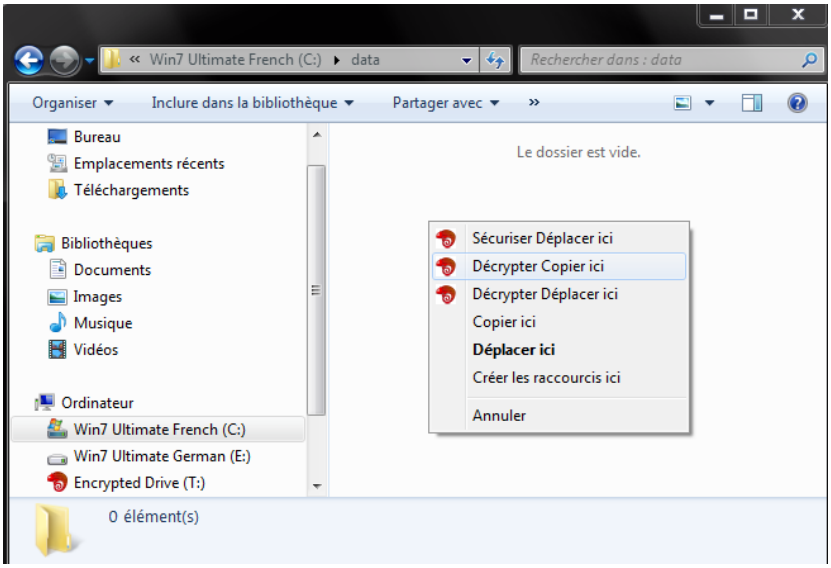
2. **Saisissez votre mot de passe (si activé)**



3. **Cliquez et maintenez appuyé le bouton droit de la souris sur le fichier .cge**

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

4. **Faites glisser le pointeur de la souris** vers le dossier cible et relâchez le bouton droit de la souris. Le contenu décrypté sera créé dans ce dossier.



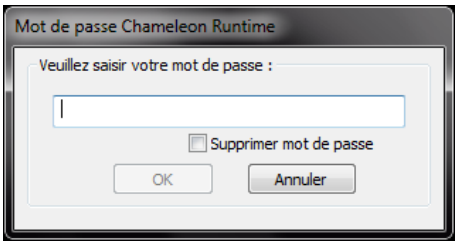
5. **Sélectionnez « Décrypter Déplacer ici» ou « Décrypter Copier ici ».**
   « Décrypter Déplacer ici» déplace le contenu décrypté vers la destination tout en supprimant le fichier .cge en sécurité. Il est conseillé d'utiliser cette méthode afin d'éviter que vos données non cryptées résident (temporairement) dans une mémoire non sécurisée ou distante.

   « Décrypter Copier ici » fait la même chose, mais sans supprimer le fichier source.

L'option Décrypter Coller est également disponible :

1. **Connectez le dispositif**

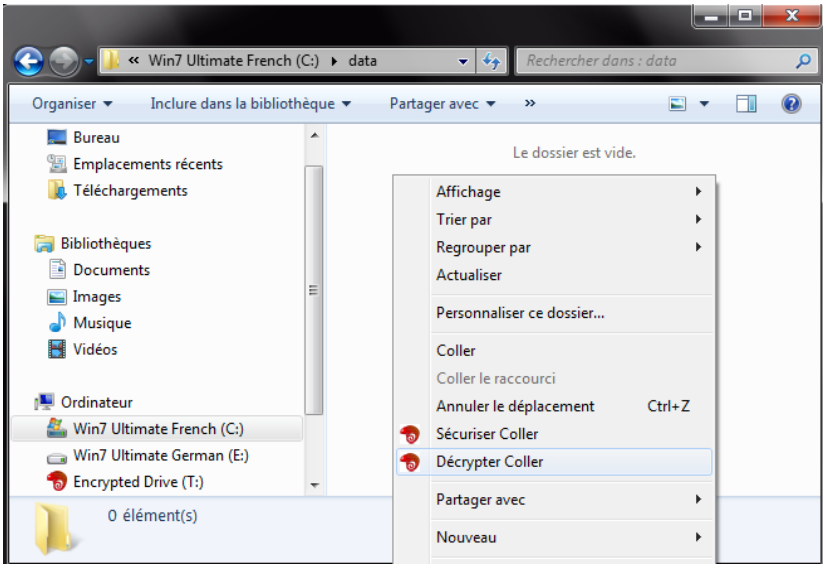
2. **Saisissez votre mot de passe (si activé)**



3. **Faites un clic droit sur fichier .cge file** à décrypter, puis **sélectionnez « Couper » ou « Copier »**. Vous pouvez également utiliser les raccourcis Couper (CTRL+x) ou Copier (CTRL+c) du clavier.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

4. **Faites un clic droit sur le disque ou répertoire de destination.**



5. **Sélectionnez « Décrypter Coller »**

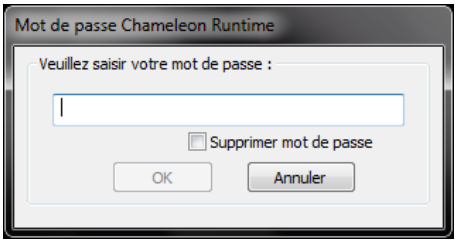
Ceci déplace le contenu décrypté vers la destination. Si « Couper » avait été sélectionné, le fichier source sera supprimé en sécurité une fois le décryptage terminé.

4.3 Voir les détails d'un fichier crypté

Pour voir les détails d'un fichier crypté :

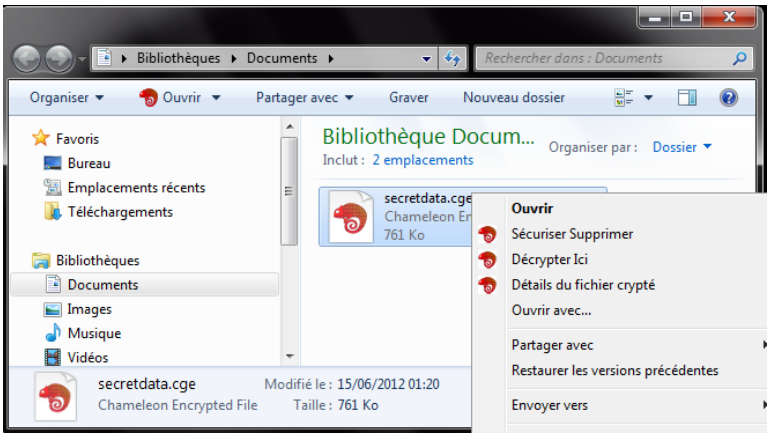
1. **Connectez le dispositif**

2. **Saisissez votre mot de passe** (si activé)



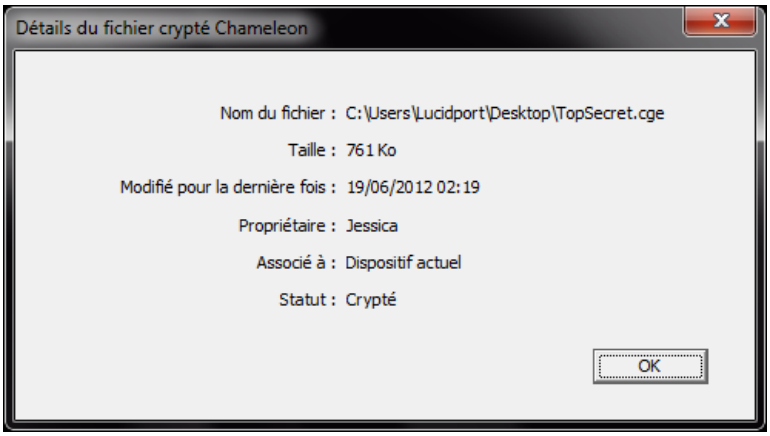
3. **Faites un clic droit sur le fichier .cge**

4. **Sélectionnez « Détails du Fichier Crypté »**



LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

1. Les détails du fichier s'affichent dans une nouvelle fenêtre


Détails du fichier crypté Chameleon
Nom du fichier : C:\Users\Lucidport\Desktop\TopSecret.cge
Taille : 761 Ko
Modifié pour la dernière fois : 19/06/2012 02:19
Propriétaire : Jessica
Associé à : Dispositif actuel
Statut : Crypté
OK

5 Dupliquer un dispositif Chameleon

Si vous perdez ou cassez votre dispositif Chameleon, les données du disque crypté peuvent être récupérées en utilisant un nouveau dispositif Chameleon et la phrase de passe de récupération que vous aviez indiquée pendant l'installation. Ce processus peut également être utilisé pour créer des doubles du dispositif Chameleon. Les Chameleon sans phrase de passe de récupération ne peuvent pas être dupliqués.

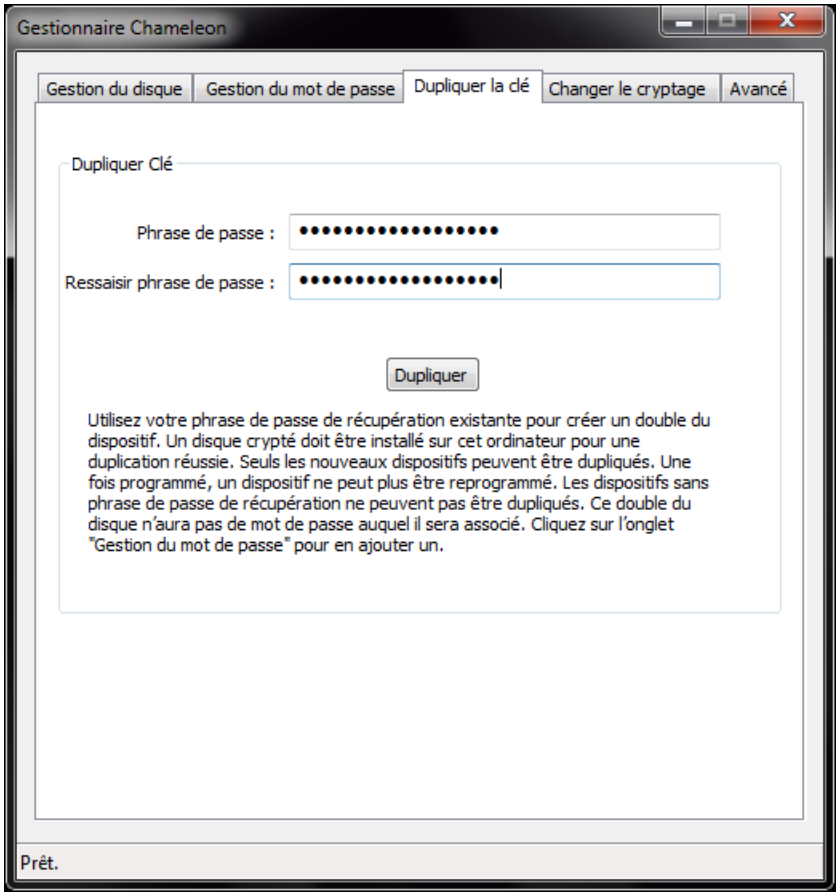
1. **Connectez un nouveau dispositif Chameleon.**

2. **Démarrez le Gestionnaire Chameleon** Cliquez sur « Démarrer » de Windows > Tous les programmes > Chameleon > Gestionnaire Chameleon

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

3. **Dans l'onglet « Dupliquer Clé », saisissez votre phrase de passe de récupération d'origine**

4. **Cliquez sur le bouton « Créer »**.


Gestionnaire Chameleon
Gestion du disque
Gestion du mot de passe
Dupliquer la clé
Changer le cryptage
Avancé
Dupliquer Clé
Phrase de passe :
Ressaisir phrase de passe :
Dupliquer
Utilisez votre phrase de passe de récupération existante pour créer un double du dispositif. Un disque crypté doit être installé sur cet ordinateur pour une duplication réussie. Seuls les nouveaux dispositifs peuvent être dupliqués. Une fois programmé, un dispositif ne peut plus être reprogrammé. Les dispositifs sans phrase de passe de récupération ne peuvent pas être dupliqués. Ce double du disque n'aura pas de mot de passe auquel il sera associé. Cliquez sur l'onglet "Gestion du mot de passe" pour en ajouter un.
Prêt.

Ce nouveau double du dispositif n'aura pas de mot de passe auquel il sera associé. Cliquez sur l'onglet« Gérer Mot de passe » pour en ajouter un.

Vous n'avez pas besoin du dispositif Chameleon d'origine pour créer un double. Mais par précaution, un disque crypté doit être présent afin d'assurer la réussite de la duplication.

6 Désactiver des dispositifs Chameleon égarés

Vous pouvez verrouiller un dispositif perdu en changeant la phrase de passe de récupération et en faisant migrer tous les disques cryptés[3] vers le nouveau dispositif. Chaque dispositif ne peut être changé qu'une seule fois. Afin de répéter cette procédure, il vous faudra un nouveau dispositif Chameleon. Par précaution, un disque crypté doit être présent afin d'assurer la réussite de la duplication.

Il vous faudra un dispositif programmé avec la phrase de passe de récupération d'origine que vous aviez spécifiée lors de l'installation. Si votre dispositif d'origine a été perdu, vous devrez préparer un remplacement. (Voir « **Error! Reference source not found.**). Votre disque dur (C:\) oit avoir assez d'espace libre pour pouvoir contenir tous les fichiers des disques cryptés. Selon le volume des données cryptées, il se peut que ce processus prenne un certain temps. Tous les

[3] Copies de sauvegarde y compris

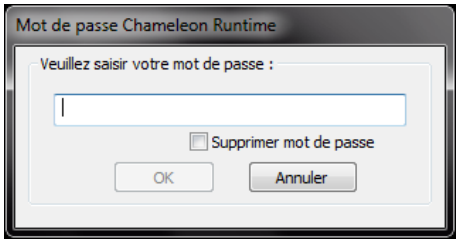
LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

disques cryptés non connectés (ainsi que les copies de sauvegarde) resteront accessibles par le dispositif d'origine/perdu. Il vous sera demandé de les faire migrer lorsqu'ils seront connectés ultérieurement

Pour changer le dispositif et faire migrer les disques cryptés :

1. **Connectez un double du dispositif Chameleon d'origine**

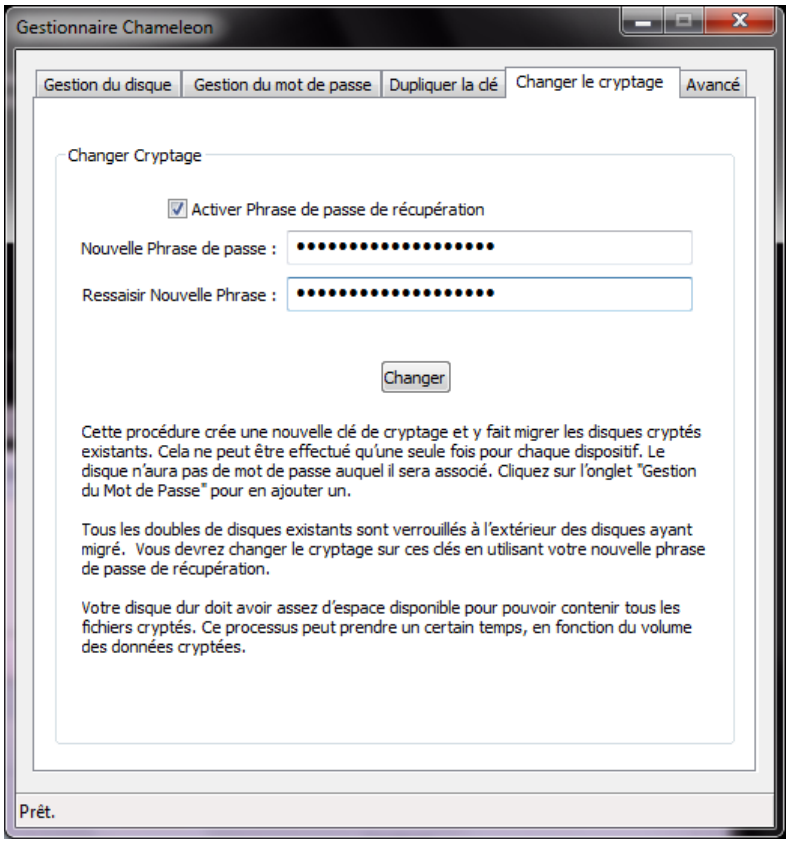
2. **Saisissez votre mot de passe** (si activé).



3. **Démarrer le Gestionnaire Chameleon**

Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Gestionnaire Chameleon

4. **Sélectionner l'onglet « Changer le cryptage »**


Gestionnaire Chameleon
Gestion du disque
Gestion du mot de passe
Dupliquer la clé
Changer le cryptage
Avancé
Changer Cryptage
Activer Phrase de passe de récupération
Nouvelle Phrase de passe :
Ressaisir Nouvelle Phrase :
Changer
Cette procédure crée une nouvelle clé de cryptage et y fait migrer les disques cryptés existants. Cela ne peut être effectué qu'une seule fois pour chaque dispositif. Le disque n'aura pas de mot de passe auquel il sera associé. Cliquez sur l'onglet "Gestion du Mot de Passe" pour en ajouter un.
Tous les doubles de disques existants sont verrouillés à l'extérieur des disques ayant migré. Vous devrez changer le cryptage sur ces clés en utilisant votre nouvelle phrase de passe de récupération.
Votre disque dur doit avoir assez d'espace disponible pour pouvoir contenir tous les fichiers cryptés. Ce processus peut prendre un certain temps, en fonction du volume des données cryptées.
Prêt.

`Saisissez la nouvelle phrase de passe de récupération.` `(Reportez-vous à « 0` Le Chameleon Pro fonctionne sur les PC équipés de Windows XP, Vista et Win7.

5. Installation » concernant le choix d'une phrase de passe de récupération)

6. **Cliquez sur "Changer"**.

Cette procédure créée des disques cryptés de remplacement en utilisant la nouvelle phrase de passe de récupération avec tous vos fichiers cryptés dessus. Le dispositif Chameleon actualisé

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

n'aura pas de mot de passe auquel il sera associé. Cliquez sur l'onglet « Gérer mot de passe » pour en ajouter un.

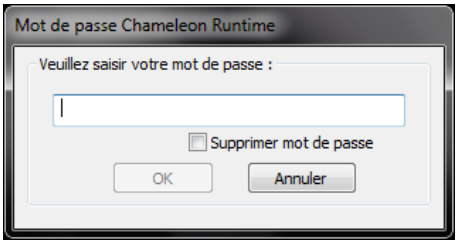
Les disques cryptés qui n'ont pas migré restent accessibles avec le nouveau dispositif Chameleon.

6.1 Faire migrer des fichiers cryptés (.cge)

En plus des disques cryptés, vous devez également recrypter les fichiers .cge qui avaient été sécurisés pas la clé de cryptage d'origine.

1. **Connectez le dispositif**

2. **Saisissez votre mot de passe** (si activé)



3. **Démarrer le « Migrator de fichiers cryptés »**

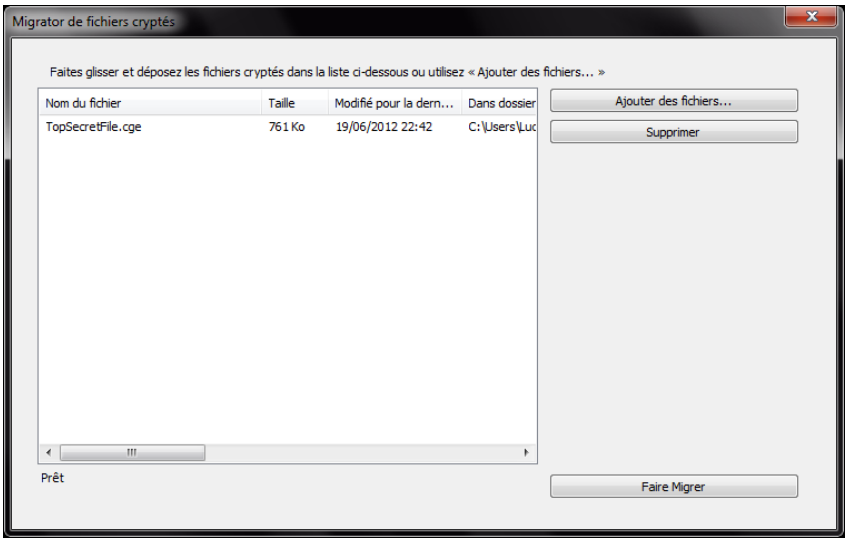
Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Migrator de Fichiers Cryptés

4. **Sélectionnez les fichiers .cge à faire migrer.**

Faites-les glisser directement vers la fenêtre contenant la liste des fichiers

ou alors

Cliquez sur « Ajouter des fichiers », naviguez et sélectionnez les fichiers.



LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

5. **Fermez tous les fichiers ouverts qui résident dans les disques cryptés.**

   Avant que le processus de migration ne commence, les disques cryptés seront détachés. Si un fichier est ouvert le Migrator demandera à l'utilisateur de le fermer.

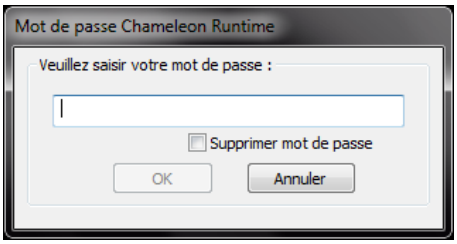
6. **Cliquez sur le bouton « Faire Migrer »**

Une fois le processus de migration terminé, le dispositif perdu n'aura plus accès au fichier crypté. Le disque dur contenant les fichiers .cge doit avoir assez d'espace libre pour pouvoir contenir une copie du fichier le plus volumineux de la liste. Selon le volume des données cryptées, il se peut que ce processus prenne un certain temps.

Vos disques cryptés seront rattachés une fois le processus de migration terminé.

7 Protection par mot de passe

Par défaut, les mots de passe ne sont pas exigés pour les dispositifs Chameleon. Cependant en ajoutant la protection par mot de passe, vous sécurisez vos données au cas où vous perdriez votre dispositif ainsi que votre PC. Une fois activé, le logiciel Chameleon exigera un mot de passe à chaque connexion ou lorsque l'ordinateur redémarre ou sort du mode veille.



Le mot de passe est différent de la phrase de passe de récupération. La phrase de passe de récupération n'est saisie que lors de l'initialisation ou d'une duplication. Une fois activé, le mot de passe doit être saisi à chaque fois que le dispositif est connecté. Il sert à empêcher tout accès non autorisé au dispositif, pas à protéger vos données. Des dispositifs ayant la même phrase de passe de récupération, mais des mots de passe différents peuvent accéder aux mêmes disques cryptés.

Si vous oubliez votre mot de passe, supprimez la protection par mot de passe en entrant votre phrase de passe de récupération dans l'invite d'entrée de mot de passe.

7.1 Modification du mot de passe

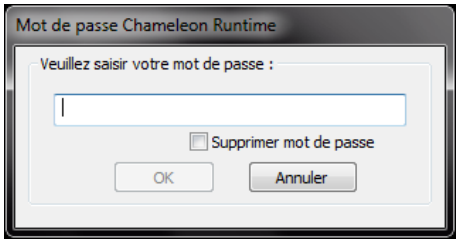
Vous pouvez ajouter, changer ou supprimer la protection par mot de passe aussi souvent que vous le souhaitez. Il est possible d'avoir des doubles de dispositifs avec des mots de passe différents (ou sans aucun de mot de passe). Sachez qu'un dispositif Chameleon sans protection par mot de passe peut accéder aux données protégées par un dispositif différent avec protection par mot de passe tant qu'ils ont la même phrase de passe de récupération.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

Pour modifier les options de mot de passe :

1. **Connectez le dispositif**

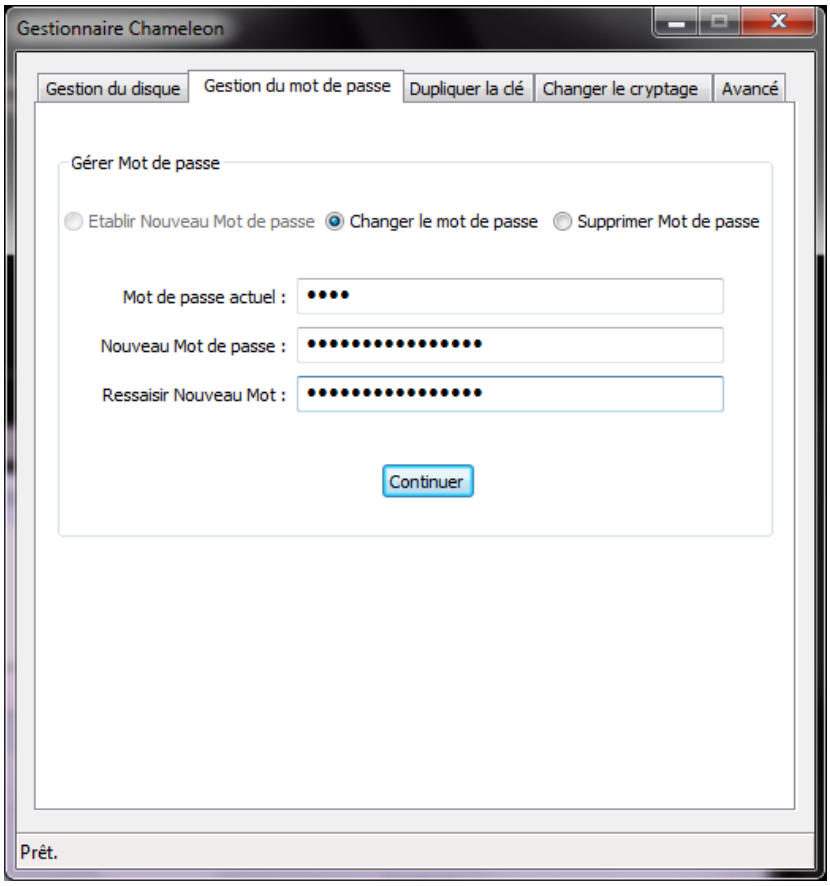
2. **Saisissez votre mot de passe (si déjà activé)**



3. **Démarrez le Gestionnaire Chameleon**

Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Gestionnaire Chameleon

4. **Sélectionnez l'onglet « Gérer Mot de Passe ».**



LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

- Pour ajouter un mot de passe, sélectionnez « Paramétrer un nouveau mot de passe » puis saisissez le nouveau mot de passe et cliquez sur le bouton « Continuer ».

- Pour changer votre mot de passe : Sélectionnez « Changer mot de passe ». Saisissez votre mot de passe actuel. Saisissez le nouveau mot de passe et vérifiez-le. Cliquez sur le bouton « Continuer ».

- Pour supprimer le mot de passe, sélectionner « Supprimer mot de passe » puis sélectionner votre mot de passe actuel et cliquez sur le bouton « Continuer ».

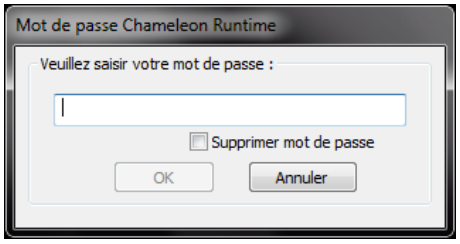
Vous pouvez changer de mot de passe aussi souvent que vous le souhaitez.

8 Ajouter, supprimer et modifier la taille des disques cryptés

Vous pouvez ajouter, supprimer ou modifier la taille des disques cryptés à n'importe quel moment. Tant qu'il y a assez d'espace sur le disque, il n'y a pas de limite au nombre de disques cryptés qui peuvent être associés à un dispositif Chameleon. Les disques cryptés peuvent être créés sur votre disque dur interne ou sur les disques USB externes.

1. **Connectez votre dispositif.**

2. **Saisissez votre mot de passe (si déjà activé)**

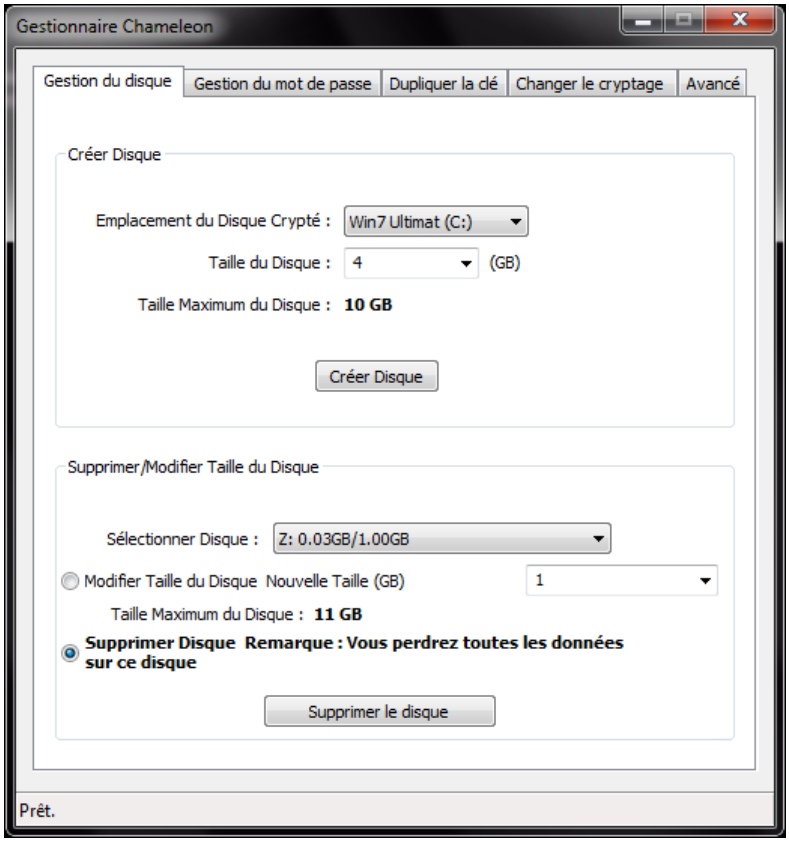


3. **Démarrez le Gestionnaire Chameleon**

Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Gestionnaire Chameleon

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

4. **Sélectionnez l'onglet « Gérer Disque ».**



- Pour ajouter un disque, indiquez la taille et l'emplacement du disque crypté, puis cliquez sur le bouton « Créer Disque ».

- Afin de supprimer un disque, sélectionnez le disque existant à partir du menu déroulant, puis sélectionnez « Supprimer Disque ». Cliquez sur le bouton « Supprimer Disque ». Il vous sera demandé de saisir une confirmation.

- Afin de modifier la taille d'un disque, sélectionnez votre disque à partir du menu déroulant, puis sélectionnez « Modifier Taille du Disque ». Saisissez la taille de votre choix, puis cliquez sur le bouton « Modifier Taille du Disque ». Lorsque vous voulez réduire la taille du disque, votre disque dur (C:\) doit avoir assez d'espace libre pour stocker temporairement le contenu entier du disque crypté.

9 Fonctions supplémentaires et restrictions

9.1 Utilisation d'un dispositif Chameleon à partir de plusieurs ordinateurs

Un dispositif Chameleon peut être utilisé sur plusieurs ordinateurs.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

Si le logiciel Chameleon n'a pas été installé, suivre les indications de la rubrique 0 "Le Chameleon Pro fonctionne sur les PC équipés de Windows XP, Vista et Win7. `Installation` " pour l'installer sur un autre ordinateur. Après l'étape 4, le logiciel d'installation passera directement à l'étape 7 pour créer un disque crypté si le dispositif a déjà été initialisé.

Si le logiciel Chameleon a déjà été installé, reportez-vous à la rubrique 2 "`Installation et réglages` " l'étape 7 pour créer un disque crypté.

9.2 Utilisation de plusieurs dispositifs Chameleon sur le même ordinateur

Vous pouvez avoir plusieurs disques cryptés associés à des dispositifs Chameleon différents sur le même ordinateur et disque dur.

Aucune installation de logiciel supplémentaire n'est nécessaire. Connectez le second dispositif et utilisez le Gestionnaire Chameleon pour créer des disques cryptés associés avec ce dispositif. A moins qu'il ne s'agisse d'un double, le second dispositif ne peut accéder qu'à ses propres disques (et pas aux disques associés avec le premier dispositif).

Dans le cas où vous ne souhaiteriez plus utiliser un certain dispositif sur un PC en particulier, supprimez ses disques cryptés en utilisant le Gestionnaire Chameleon plutôt que de désinstaller le logiciel Chameleon. En désinstallant le logiciel Chameleon vous ne supprimez pas les disques cryptés.

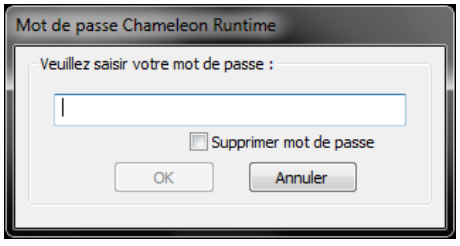
Le logiciel Chameleon ne permet pas d'insérer plus d'un dispositif Chameleon à la fois.

9.3 Fichier Windows de Pagination

Windows peut stocker des données temporaires dans son fichier de pagination (mémoire virtuelle). Ce fichier est généralement non crypté et est réactualisé continuellement. Activez le cryptage pagefile pour indiquer à Windows de crypter son fichier de pagination.
Pour activer le cryptage pagefile:

1. **Connectez le dispositif.**

2. **Saisissez votre mot de passe (si déjà activé)**



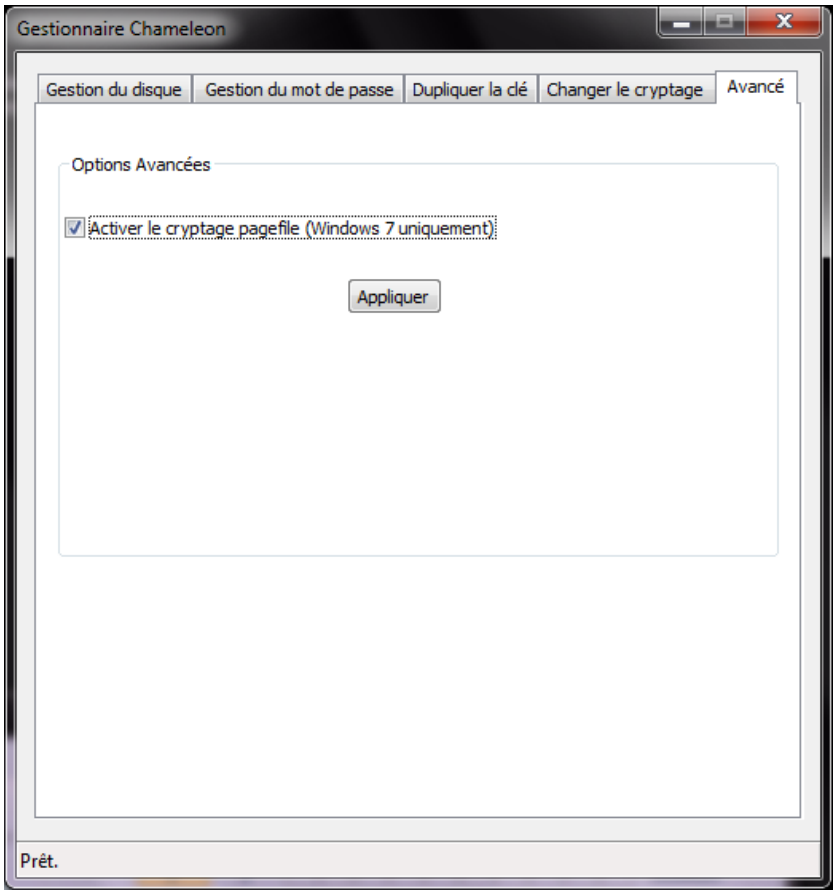
3. **Démarrez le Gestionnaire Chameleon**

Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Gestionnaire Chameleon

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

4. **Sélectionnez l'onglet « Avancé »**

5. **Sélectionnez « Activer Cryptage Pagefile »** puis **cliquez sur « Appliquer »**



Le cryptage du fichier de pagination élimine toute faille de sécurité potentielle, mais ralentit légèrement l'ordinateur. Seul Windows 7 permet le cryptage page file (ignoré pour les autres systèmes d'exploitation).

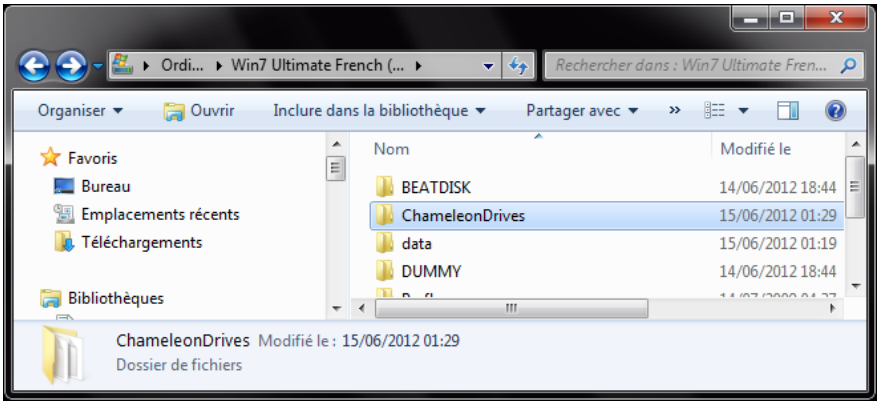
9.4 Retirer le dispositif de façon sécurisée

Un débranchement du dispositif alors que des données sont en cours d'écriture au disque crypté peut entraîner la corruption de ces données. Cette situation serait similaire à la déconnexion d'un disque dur externe alors qu'il serait en cours d'écriture. Afin d'être absolument certain qu'il n'y ait pas d'écriture en cours, utilisez la fonction « Retirer le périphérique en toute sécurité » de Windows avant de déconnecter le dispositif.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

9.5 Créer des copies de sauvegarde des données

Pour créer des copies de sauvegarde des disques cryptés, copiez le répertoire ChameleonDrives dans un autre emplacement. Ce répertoire se trouve dans le haut niveau de votre disque dur (par ex : C:\ChameleonDrives\). Puisque les disques cryptés sont toujours cryptés, les copies de sauvegarde restent protégées. Il ne faut pas connecter le dispositif Chameleon pendant la création de copies de sauvegarde de vos données.



Vous pouvez ajouter le répertoire ChameleonDrives à la liste des copies de sauvegarde prévues.

AVERTISSEMENT : Ne copiez pas la sauvegarde du répertoire ChameleonDrives sur le haut niveau (racine) d'un disque (par ex : D:\ChameleonDrives). Le logiciel Chameleon n'est pas capable de distinguer l'original de sa copie. Si des disques identiques sont détectés dans le haut niveau, le logiciel Chameleon n'activera aucun des disques. Tous les sous-répertoires et emplacements réseau fonctionneront (par ex : D:\backup\ChameleonDrives).

10 Garantie limitée et Mentions Légales

Chameleon
Copyright (c) 2011, LucidPort Technology, Inc.
485 E. Evelyn Ave
Sunnyvale, CA 94086
USA
Tél: (001) 408 720 8800
Fax: (001) 408 720 8900

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

Veuillez contacter support@marathon6.com pour toute question technique.
Contactez sales@marathon6.com pour des renseignements concernant les ventes ou la garantie.
Visitez http://www.marathon6.com/chameleon pour les dernières mises à jour.

LucidPort Technology, Inc. garantit son produit contre tout défaut de matériel ou de fabrication dans des conditions normales d'utilisation et d'entretien pendant une période de un (1) année à partir de la date d'achat. La seule obligation de LucidPort Technology, Inc. relativement aux réclamations de non-conformité pendant la période de garantie décrite plus haut sera, à sa discrétion, de réparer ou de remplacer tout article de les produits.

Les obligations de garantie de LucidPort Technology, Inc. aux termes de la présente section dépendent expressément du respect des conditions qui suivent : (i.) les produits doivent être installés, utilisés et entretenus correctement en tout temps par le client; (ii.) les produits ne doivent pas être soumis à des contraintes mécaniques inhabituelles ou à des conditions environnementales ou électriques inhabituelles ou à d'autres forces majeures; (iii.) les produits ne doivent pas être soumis à une mauvaise utilisation, à un accident ou à une installation/désinstallation non autorisée par le client ou par un tiers; (iv.) les produits ne doivent pas être modifiés ou altérés d'une manière non autorisée, sauf approbation écrite ou intervention de LucidPort Technology, Inc. ; et (v.) le client doit installer rapidement toutes les mises à jour de produits publiées pour ces produits par LucidPort Technology, Inc. pendant la durée de la garantie. LucidPort Technology, Inc. ne garantit pas que les produits fonctionneront dans toute combinaison d'utilisation spécifique qui pourrait être choisie par le client ni que les produits fonctionneront sans interruption ou sans erreur ni que tous les défauts ou non-conformités seront corrigés. En outre, LucidPort Technology, Inc. n'aura aucune obligation de garantie pour toute défaillance de produits qui ne se conforment pas aux spécifications de produits applicables découlant de la combinaison d'un produit avec un matériel et/ou un logiciel non fourni par LucidPort Technology, Inc.

LucidPort Technology, Inc. décline toute responsabilité pour tout dommage ou toute perte de programmes, données ou autres renseignements sauvegardés sur tout support dans le matériel LucidPort Technology, Inc. ou tout produit extérieur à LucidPort Technology, Inc. ou toute pièce non couverte par la présente garantie. La récupération ou la réinstallation des programmes, données ou autres renseignements n'est pas couverte aux termes de la présente garantie limitée.

LucidPort Technology, Inc. décline toute responsabilité dans le cas d'une vente non autorisée ou d'une représentation trompeuse par des tiers revendeurs non autorisés. Les garanties LucidPort Technology, Inc. ne sont pas cessibles avec la propriété. Les produits achetés lors d'encans, ventes-débarras, marchés aux puces ou à titre d'appareils de démonstration peuvent ne pas être couverts aux termes de la présente garantie LucidPort Technology, Inc.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

The AES encryption technology in the Chameleon is classified by the United States government as an ECCN 5A002 item and can be exported under License Exception ENC, Sec. 740.17 (b)(3) of the Export Administration Regulations ("EAR"). The Chameleon may not be used or otherwise exported or re-exported into (or to a national or resident of) Cuba, Iran, North Korea, Sudan, or Syria. No further approvals or authorizations from the US government are required.

LucidPORT
Copyright © LucidPort Technology, Inc.
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com